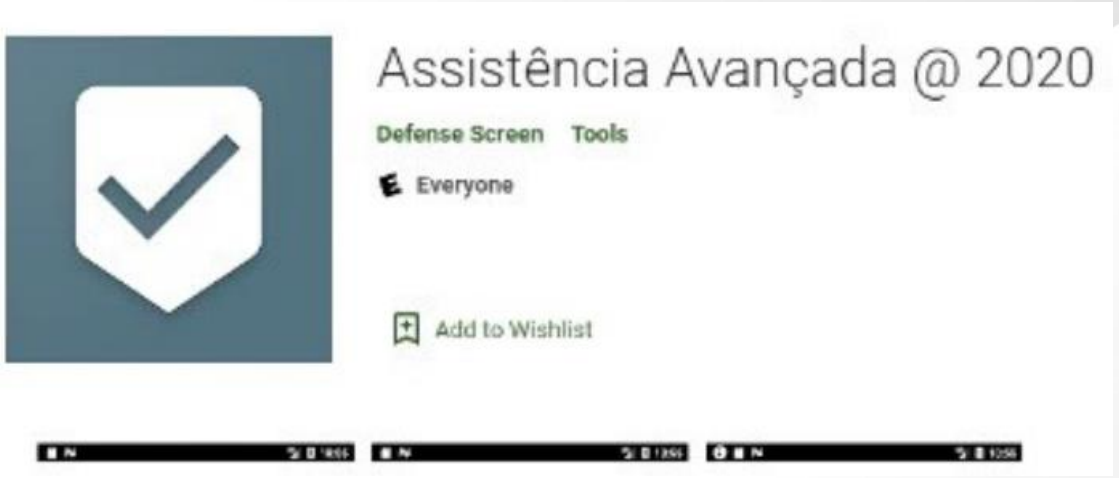
BOLETÍN NRO. 7 DE NOTICIAS Y NOVEDADES DE

SEGURIDAD INFORMÁTICA

¡Entérate! 'BRATA', el malware bancario de Android que roba tu dinero y restablece de fábrica el teléfono

Este método puede habilitarse en plataformas como correo electrónico, redes sociales, sistemas informáticos, entre otros. Puede llegar a ser incómodo para algunos usuarios, pero actualmente este método es una de las mejores opciones para contrarrestar los accesos no autorizados y ataques informáticos a nuestra información digital.



Tomado y adaptado de: https://www.xatakandroid.com/seguridad/brata-peligroso-troyano-que-se-descarga-google-play-puede-controlar-tu-android/

BOLETÍN NRO. 7 DE NOTICIAS Y NOVEDADES DE

SEGURIDAD INFORMÁTICA

¿SABIAS QUE EN LA UNIVERSIDAD DE SANTANDER ES POSIBLE HABILITAR MULTIFACTOR DE AUTENTICACIÓN PARA ACCEDER A TU CORREO ELECTRÓNICO INSTITUCIONAL?

Una de las herramientas más utilizadas por la comunidad académico administrativas en la Universidad de Santander es la Suit de office 365, en donde los usuarios acceden a su correo electrónico, almacenamiento de archivos (OneDrive), herramienta par encuentros virtuales (Teams), asistente para construcción de formularios, herramientas de ofimática, entre otros.

El acceso a estos recursos se realiza utilizando un usuario y una contraseña, la cual es asignada a cada usuario de forma exclusiva por el área de Infraestructura Tecnológica, esta seguridad se puede reforzar habilitando Multifactor de Autenticación (MFA), para lo cual los usuarios interesados en habilitar dicha característica para mejorar la seguridad de su información deben solicitarlo al área de infraestructura tecnológica dirigido al Ingeniero Alexis Palomino (alexis.palomino@udes.edu.co) o por solicitud en mesa de ayuda de Gestión TIC (helpdesk.udes.edu.co)

Universidad de Santander
Personería Jur. 810 de 12/03/96 Min.Educación UDES

BOLETÍN NRO. 7 DE NOTICIAS Y NOVEDADES DE

SEGURIDAD INFORMÁTICA

!Entérate! GOOGLE ACTIVARÁ MULTIFACTOR DE AUTENTICACIÓN (MFA) ANTES DE QUE ACABE EL AÑO

Una de las redes sociales más conocida y utilizada en el mundo, es la Suit de Google, un porcentaje importante de usuarios utilizan dicha plataforma como su aplicación de correo personal y herramientas de colaboración tales como: Drive, meet, gestor de documentos y otros.

Recientemente, este gigante de la red ha anunciado que activará el MFA de forma obligatoria paulatinamente; este proceso es muy sencillo, pero ciertamente requiere un pequeño esfuerzo adicional por parte del usuario, que tendrá que introducir el PIN que ha recibido por SMS o por una aplicación como Google Authenticator para la validación y aprobación de acceso.

Tomado y adaptado de: http://unaaldia.hispasec.com.

Universidad de Santander
Personería Jur. 810 de 12/03/96 Min.Educación UDES

BOLETÍN NRO. 7 DE NOTICIAS Y NOVEDADES DE

SEGURIDAD INFORMÁTICA

!ALERTA! APLICACIÓN PDF+ CATALOGADA COMO TROYANO BANCARIO

PDF+ una de las aplicaciones más descargadas en Google Play para la edición de archivos PDF, fue identificada como una plataforma con código malicioso para realizar ataques cibernéticos; esta aplicación que fue deshabilitada en Google Play estaba ubicada en la parte alta de la lista de descargas superando las 10.000.

El virus troyano bancario que contenía la aplicación permite controlar la pantalla y acceder a los contactos, SMS y datos almacenados en el celular que pueden servir para desocupar las cuentas bancarias de las personas que la instalaron.

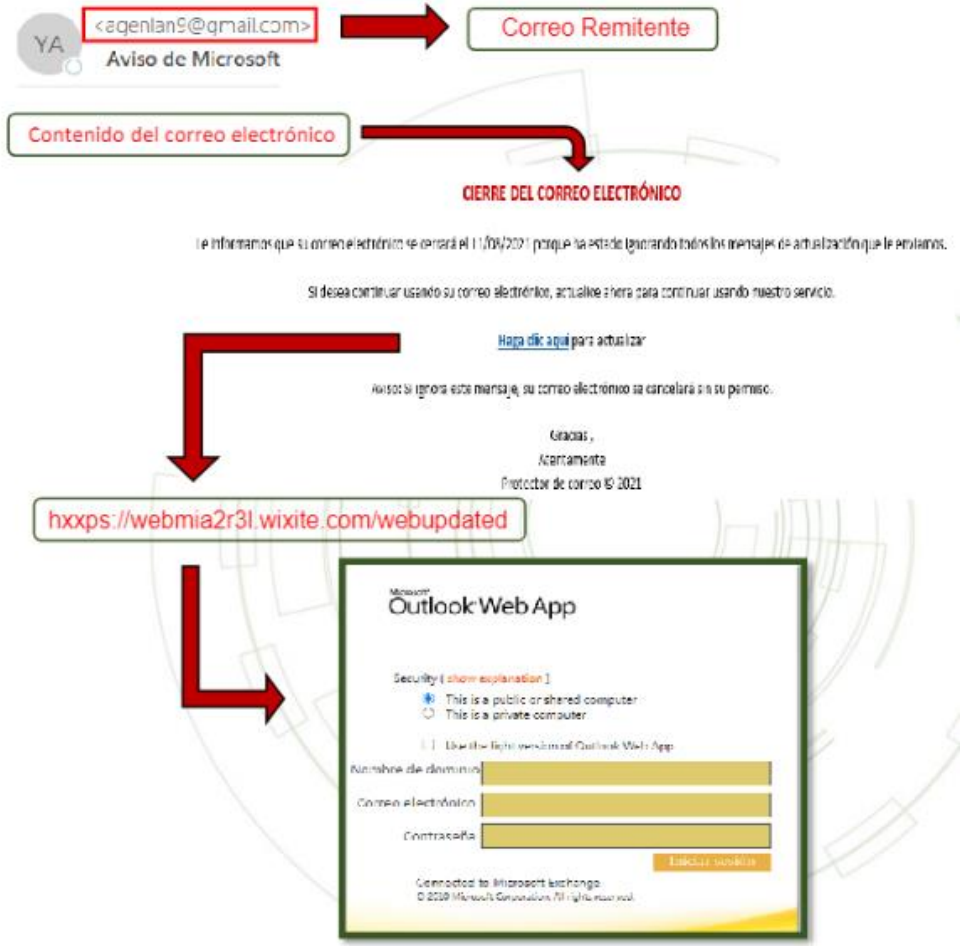
Tomado y adaptado de: https://www.elespectador.com/tecnologia/no-la-instale-la-aplicacion-que-es-un-troyano-bancario-y-roba-todos-sus-datos/

Universidad de Santander
Personería Jur. 810 de 12/03/96 Min.Educación UDES

BOLETÍN NRO. 7 DE NOTICIAS Y NOVEDADES DE

SEGURIDAD INFORMÁTICA

!Alerta! Web Spoofing



Se encuentra circulando en la red un correo electrónico falso, en el cual envían una supuesta notificación de cierre de correo electrónico, en su contenido se encuentra el siguiente enlace (hxxps://webmia2r3l.wixite.com/webupdated). Al acceder al enlace mencionado, el usuario es dirigido a una pagina falsa similar a la de Microsoft Outlook web App, con el propósito de realizar el robo de credenciales de acceso a su buzón y datos personales.

Si recibe este o alguno otro tipo de correo sospechoso, por favor informar al área de Seguridad Informática (seguridadinformatica@udes.edu.co) para realizar la validación y tratamiento si es requerido.

Tomado y adaptado dehttps://cc-csirt.policia.gov.co/alertas-tips/2021/4to-trimestre/boletin-informativo-no-022-alerta-de-web-spoofing

Universidad de Santander
Personería Jur. 810 de 12/03/96 Min.Educación UDES